ELSEVIER

Theoretical Computer Science 235 (2000) 71–88

Theoretical Computer Science

www.elsevier.com/locate/tcs

Peter Bürgisser *

Institut für Mathematik, Universität Zürich, Winterthurerstr. 190, CH-8057 Zürich, Switzerland

Dedicated to Manuel Blum on the occasion of his 60th birthday

Abstract

Valiant developed a nonuniform algebraic analogue of the theory of NP-completeness for computations with polynomials over a field k in (Valiant, Proceedings of the 11th ACM STOC, 1979, pp. 249–261; Logic Algorithmic: An International Symposium held in honor of Ernst Specker, Vol. 30, 1982, pp. 365–380). This theory centers around his hypothesis $\mathrm{VP}_k \neq \mathrm{VNP}_k$, the analogue of Cook's hypothesis P $\neq$ NP. We identify the Boolean parts of Valiant's algebraic complexity classes VP_k and VNP_k as familiar nonuniform complexity classes. As a consequence, we obtain rather strong evidence for Valiant's hypothesis: if it were wrong, then the nonuniform versions of NC and PH would be equal. In particular, the polynomial hierarchy would collapse to the second level. We show this for fields of characteristic zero and finite fields; in the first case we assume a generalized Riemann hypothesis. The crucial step in our proof is the elimination of constants in k, which relies on a recent method proposed by Koiran [16].

Keywords: Algebraic complexity; NP-completeness; Elimination of constants; Reduction modulo primes

1. Introduction

In [22, 25] Valiant developed an algebraic analogue of the theory of NP-completeness, which grew out of his studies of enumeration problems and led to the concept of #P-completeness [23, 24]. This algebraic theory seems to be most natural for discussing complexity question for polyomials. But also for investigating structural questions in complexity theory, the algebraic (or arithmetic) approach has proved to be useful (compare Babai and Fortnow [2]).

* Corresponding address: Hardstreet 16, 5430 Wettingen, Switzerland.
E-mail address: buerg@amath.unizh.ch (P. Bürgisser)

0304-3975/00/$ - see front matter
PII: S0304-3975(99)00183-8

In the sequel we briefly recall the main features of Valiant's algebraic model. For detailed expositions see von zur Gathen [10], Bürgisser et al. [7, Chapter 21], and Bürgisser [5].

A *p-family* over a fixed field k is a sequence $f=(f_n)$ of multivariate polynomials $f_n \in k[X_1,\ldots,X_{v(n)}]$ such that the functions $n \mapsto v(n)$ and $n \mapsto \deg f_n$ are *p-bounded*, i.e., majorized by a polynomial. An important example is the *permanent family* $\mathrm{PER}=(\mathrm{PER}_n)$, where PER_n is the permanent of an n by n matrix with distinct indeterminate entries.

Let $L(f_n)$ denote the (total) complexity of $f_n \in k[X_1,\ldots,X_{v(n)}]$, that is, the minimum number of arithmetic operations $+,-,*$ to compute f_n from the variables X_i and constants in k by a straight-line program (or arithmetic circuit). We call a p-family *p-computable* iff $n \mapsto L(f_n)$ is p-bounded. The p-computable families constitute the complexity class VP_k. We remark that the restriction to p-bounded degrees is a severe one: although X^{2^n} can be computed with only n multiplications, the corresponding sequence is not considered to be p-computable, as the degrees grow exponentially.

A p-family is called *p-definable* iff there exists a p-computable family $g=(g_n)$ with $g_n \in k[X_1,\ldots,X_{u(n)}]$ such that for all n

$$f_n(X_1,\ldots,X_{v(n)}) = \sum_{e\in\{0,1\}^{u(n)-v(n)}} g_n(X_1,\ldots,X_{v(n)},e_{v(n)+1},\ldots,e_{u(n)}).$$

The set of p-definable families form the complexity class VNP_k. Obviously, $\mathrm{VP}_k \subseteq \mathrm{VNP}_k$, and *Valiant's hypothesis* claims that this inclusion is strict. We can consider this as an algebraic counterpart of the well-known hypothesis $\mathrm{P} \neq \mathrm{NP}$ due to Cook [8].

We will employ a very simple and restrictive notion of reduction. A polynomial f_n is called a *projection* of a polynomial $g_m \in k[X_1,\ldots,X_u]$, $f_n \leqslant g_m$, iff $f_n(X_1,\ldots,X_{v(n)}) = g_m(a_1,\ldots,a_u)$ for some $a_i \in k \cup \{X_1,\ldots,X_{v(n)}\}$. That is, f_n can be derived from g_m through substitution by indeterminates and constants. A p-family $f=(f_n)$ is called a *p-projection* of $g=(g_m) \in \mathrm{VNP}_k$ iff there is a p-bounded $t:\mathbb{N}\to\mathbb{N}$ such that f_n is a projection of $g_{t(n)}$ for all n. Finally, a p-family $g \in \mathrm{VNP}$ is called *VNP_k-complete* iff any $f \in \mathrm{VNP}_k$ is a p-projection of g.

In [22] Valiant obtained the remarkable result that the permanent family (if $\mathrm{char}\, k \neq 2$) and the family of Hamilton cycle polynomials are VNP-complete. It turns out that the "generating functions" corresponding to several other NP-complete graph problems like Cliques, factors, Hamilton cycles in planar graphs etc. yield VNP-complete families as well (cf. [5]). Quite astonishingly, there exist *specific* families in VNP_k over finite fields k, which are neither VNP_k-complete nor p-computable, provided the polynomial hierarchy does not collapse (see [5, 6]).

The goal of this paper is to establish close relations between Valiant's algebraic model and discrete complexity theory based on the computational model of Turing machines. In particular, we will show that Valiant's hypothesis is a consequence of standard hypotheses in discrete complexity theory.

We assign now to the algebraic classes VP_k and VNP_k their "Boolean parts" which consist of certain string functions $\{0,1\}^* \to \{0,1\}^*$. Let $f=(f_n)$ be a p-family over k such that $f_n \in k[X_1,\ldots,X_n]$. If $\operatorname{char} k=0$, we assume that $f_n(x)$ is a natural number of bitsize $n^{\mathrm{O}(1)}$ for all $x\in\{0,1\}^n$. If $\operatorname{char} k=p>0$, we assume that the coefficients of f_n are contained in the prime field $\mathbb{F}_p$ of k. We define the Boolean part of such an f as the string function which maps $x\in\{0,1\}^n$ to the binary encoding of $f_n(x)$. The Boolean part $\mathrm{BP}(\mathrm{VP}_k)$ of VP_k is the set of the Boolean parts of all $f\in\mathrm{VP}_k$ for which it is defined. The Boolean part $\mathrm{BP}(\mathrm{VNP}_k)$ is defined analogously.

Our main result identifies the Boolean parts of VP_k and VNP_k as familiar nonuniform complexity classes. (For definitions of these classes see Section 2.) (GRH) denotes the generalized Riemann hypothesis for number fields (cf. Section 4).

Theorem 1.1. 1. *Under* (*GRH*) *we have for fields* k *of characteristic zero*

$$\mathrm{FNC}^1/\mathrm{poly} \subseteq \mathrm{BP}(\mathrm{VP}_k) \subseteq \mathrm{FNC}^3/\mathrm{poly},$$

$$\#\mathrm{P}/\mathrm{poly} \subseteq \mathrm{BP}(\mathrm{VNP}_k) \subseteq \mathrm{FP}^{\#\mathrm{P}}/\mathrm{poly}.$$

2. *For finite fields of characteristic* p *we have*

$$\mathrm{FNC}^1/\mathrm{poly} \subseteq \mathrm{BP}(\mathrm{VP}_k) \subseteq \mathrm{FNC}^2/\mathrm{poly}, \quad \#_p\mathrm{P}/\mathrm{poly} = \mathrm{BP}(\mathrm{VNP}_k)\ .$$

The main difficulty in proving this theorem comes from the fact that Valiant's model allows the use of arbitrary constants in k. Assume we had a straight-line program Γ_n of polynomial size, which computes the permanent $\operatorname{per}(A)$ of a given matrix A using some complex constants. In order to transform Γ_n into a polynomial size Boolean circuit which computes the permanent of 0,1-matrices, we would have to replace the complex constants by something discrete of small size. In fact, we can show that for each n there is a large prime number $p_n > n!$ of polynomial bitsize, and that there are constants in $\mathbb{F}_{p_n}$, such that the simulation of Γ_n on these constants in $\mathbb{F}_{p_n}$ computes $\operatorname{per}(A) \bmod p_n = \operatorname{per}(A)$. This strategy works due to our Theorem 4.1 stating that a system of integer polynomial equations, which is solvable over the complex numbers, is also solvable over many finite fields $\mathbb{F}_p$. This is an improvement of Theorem 8 in Koiran [16], which we think is of considerable interest in its own right.

A second ingredient of the proof is Valiant et al.'s [26] efficient parallelization of straight-line programs (Theorem 2.5).

Our main Theorem 1.1 is related to similar investigations in the realm of the BSS-model [4], where one also tries to identify the Boolean parts of certain nondiscrete complexity classes (see Koiran [15], Blum et al. [3], and Cucker and Grigoriev [9]). There also, the "elimination of constants" is the main difficulty. The absence of uniformity conditions and the fact that only straight-line computations (no branching) are considered, form the major differences between Valiant's model and the BSS-model.

Corollary 1.2. 1. *We assume (GRH). If Valiant's hypothesis were false over a field of characteristic zero, then we had*

$$\mathrm{NC}^3/\mathrm{poly} = \mathrm{P}/\mathrm{poly} = \mathrm{NP}/\mathrm{poly} = \mathrm{PH}/\mathrm{poly}$$

and $\#\mathrm{P}/\mathrm{poly} = \mathrm{FP}/\mathrm{poly}$.

2. *If Valiant's hypothesis were false over a finite field k of characteristic p, then we had*

$$\mathrm{NC}^2/\mathrm{poly} = \mathrm{P}/\mathrm{poly} = \mathrm{NP}/\mathrm{poly} = \mathrm{Mod}_p\mathrm{NP}/\mathrm{poly} = \mathrm{PH}/\mathrm{poly}.$$

In both situations, the polynomial hierarchy would collapse to the second level.

To conclude this corollary from Theorem 1.1 over finite fields, we use Theorem 3.1, which is obtained by combining a technique of Valiant and Vazirani [27] with Adleman's trick [1]. The statement about the possible collapse of the polynomial hierarchy follows from a well-known result of Karp and Lipton [13].

We conjecture that Theorem 1.1 can be strengthened to $\#\mathrm{P}/\mathrm{poly} = \mathrm{BP}(\mathrm{VNP}_k)$.

Problem. Can similar conclusions be drawn for infinite fields of positive characteristic?

2. Preliminaries

In the sequel (φ_n) will stand for a sequence of Boolean functions

$$\varphi_n : \{0,1\}^n \to \{0,1\}^{m(n)}, \quad x \mapsto (\varphi_{n,1}(x), \ldots, \varphi_{n,m(n)}(x)) \ .$$

This defines the function $\varphi : \{0,1\}^* \to \{0,1\}^*$, $x \in \{0,1\}^n \mapsto \varphi_n(x)$, having the property that the length of $\varphi(x)$ depends only on the length $n = |x|$ of x. We will call such φ *string functions* and identify them with (φ_n).

Let us recall the definition of some complexity classes. (For a survey of complexity classes see Johnson [12].)

- FP denotes the class of all string functions which can be computed by a polynomial time Turing machine.
- FNC^i is the class of string functions which can be computed by log-space uniform families of Boolean circuits of polynomial size and depth $\mathrm{O}(\log^i n)$.
- #P consists of the functions $\phi : \{0,1\}^* \to \mathbb{N}$ for which there exists a polynomial-time nondeterministic Turingmachine M such that $\phi(x)$ equals the number of accepting computations of M on x for all $x \in \{0,1\}^*$. These are exactly the functions ϕ of the form $\phi(x) = \#\{y \mid (x,y) \in R\}$, where $R \subseteq \{0,1\}^* \times \{0,1\}^*$ is a string relation decidable in polynomial time such that there is p-bounded function $t : \mathbb{N} \to \mathbb{N}$ satisfying $|y| \leqslant t(|x|)$ for all $(x,y) \in R$.
- $\mathrm{FP}^{\#\mathrm{P}}$ is the class of string functions computable in polynomial time using an oracle in #P.

- Let p be a prime number. $\#_p\mathrm{P}$ consists of the functions $\psi:\{0,1\}^* \to \mathbb{F}_p$, $x \mapsto \phi(x) \bmod p$, where ϕ is a function in #P.

The corresponding complexity classes P and NC^i of languages are obtained by restricting attention to string functions of the form $\varphi:\{0,1\}^* \to \{0,1\}$. The class NP consists of the languages $\{x \in \{0,1\}^* \mid \phi(x) \geqslant 1\}$, whereas $\mathrm{Mod}_p\mathrm{NP}$ is the set of languages $\{x \in \{0,1\}^* \mid \phi(x) \equiv 1 \bmod p\}$, where $\phi \in \#\mathrm{P}$. Finally, PH denotes the class of languages in the polynomial hierarchy (cf. [12]).

In the sequel, it will be useful to consider the elements of #P and $\#_p\mathrm{P}$ as string functions by identifying natural numbers or elements of $\mathbb{F}_p$ with their binary encoding. More specifically, a string function (φ_n) will be considered as an element of #P iff the map $\{0,1\}^* \to \mathbb{N}$ sending $x \in \{0,1\}^n$ to $\sum_{i=1}^{m(n)} \varphi_{n,i}(x)2^{i-1}$ is contained in #P. Similarly, (φ_n) is considered as an element of $\#_p\mathrm{P}$ iff $m(n) = \lfloor \log p \rfloor + 1 =: m$ for all n and the map

$$\{0,1\}^* \to \mathbb{F}_p, \quad x \mapsto \sum_{i=1}^{m} \varphi_{|x|,i}(x)2^{i-1} \bmod p$$

is contained in $\#_p\mathrm{P}$.

Using this identification, we have the obvious chain of inclusions

$$\mathrm{FNC}^1 \subseteq \mathrm{FNC}^2 \subseteq \cdots \subseteq \mathrm{FP} \subseteq \#\mathrm{P}.$$

For any complexity class $\mathscr{C}$ of string functions we may define the corresponding *nonuniform* complexity class $\mathscr{C}/\mathrm{poly}$ as follows (cf. Karp and Lipton [13]). Let $\{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$, $(x,y) \mapsto \langle x,y \rangle$ be the pairing function obtained by duplicating each bit of x and y and inserting 01 in between. A *polynomial advice* is a function $\alpha:\mathbb{N} \to \{0,1\}^*$ such that $n \mapsto |\alpha(n)|$ is p-bounded. The class $\mathscr{C}/\mathrm{poly}$ now consists of all string functions ψ of the form

$$\psi(x) = \varphi(\langle x, \alpha(|x|) \rangle),$$

where $\varphi \in \mathscr{C}$ and α is some polynomial advice function.

It is well known that FP/poly is the class of string functions which can be computed by families of Boolean circuits of polynomial size. If we additionally require that the nth circuit has depth $\mathrm{O}(\log^i n)$, we get the class $\mathrm{FNC}^i/\mathrm{poly}$.

Finally, we give a detailed definition of the notion of Boolean parts.

Definition 2.1. 1. Let (f_n) be a p-family with $f_n \in k[X_1,\ldots,X_n]$. A string function (φ_n) is called a *Boolean part* of (f_n) if we have

(a) in the case $\mathrm{char}\, k = 0$: $m(n) = n^{\mathrm{O}(1)}$ and

$$\forall x \in \{0,1\}^n\colon\ f_n(x) = \sum_{i=1}^{m(n)} \varphi_{n,i}(x)2^{i-1}\ ,$$

(b) in the case $\mathrm{char}\, k = p > 0$: $m(n) = m := \lfloor \log p \rfloor + 1$ and

$$\forall x \in \{0,1\}^n\colon\ f_n(x) = \sum_{i=1}^{m} \varphi_{n,i}(x)2^{i-1} \bmod p\ .$$

2. The *Boolean part* $\mathrm{BP}(\mathrm{VP}_k)$ of VP_k is defined as the set of all Boolean parts of p-computable families over k. The Boolean part $\mathrm{BP}(\mathrm{VNP}_k)$ is defined as the set of all Boolean parts of p-definable families over k.

Remark 2.2. Let (f_n) be a p-family with $f_n \in k[X_1,\ldots,X_n]$.
1. If $\mathrm{char}\, k = p > 0$, then the family (f_n) has a Boolean part (φ_n) iff all f_n have coefficients in the prime field $\mathbb{F}_p$. In this case (φ_n) is unique. We remark that the restriction to the prime field is just for convenience and not essential in the sequel.
2. If $\mathrm{char}\, k = 0$, then the family (f_n) has a Boolean part if $f_n(x)$ are natural numbers of bitsize n^c for all $x \in \{0,1\}^n$ and some constant c. In this case, (f_n) has infinitely many Boolean parts (leading zeros).

The following two simple lemmas will be useful later on.

Lemma 2.3. *Let* (φ_n) *be in* FP/poly *and* $u : \mathbb{N} \to \mathbb{N}$ *be* p*-bounded such that* $n < u(n)$. *We set for* $x \in \{0,1\}^n$

$$\psi_n(x) := \sum_{i,e} \varphi_{u(n),i}(x_1,\ldots,x_n,e_{n+1},\ldots,e_{u(n)})\, 2^{i-1} \ ,$$

where the sum is over all $1 \leqslant i \leqslant m(u(n))$ *and* $e \in \{0,1\}^{u(n)-n}$. *Then* (ψ_n) *is in* #P/poly.

Proof. We set $\tilde{m}(n) := m(u(n))$. Consider the set R_n consisting of the tupels (x,y,z,e) in $\{0,1\}^n \times \{0,1\}^{\tilde{m}(n)} \times \{0,1\}^{\tilde{m}(n)} \times \{0,1\}^{u(n)-n}$ satisfying for some $0 \leqslant i < \tilde{m}(n)$:

$$\begin{aligned} &y = (0,\ldots,0,1,0,\ldots,0) && \text{(the 1 at position } i\text{)} \\ &z = (z_1,\ldots,z_{i-1},0,\ldots,0) && \text{for some } z_1,\ldots,z_{i-1} \in \{0,1\} \\ &\varphi_{u(n),i}(x,e) = 1 \end{aligned}$$

The union R of the sets R_n over all $n \in \mathbb{N}$ is obviously decidable in nonuniform polynomial time. We have

$$\#\{(y,z,e) \mid (x,y,z,e) \in R\} = \sum_i \sum_e \varphi_{u(n),i}(x,e)\, 2^{i-1} = \psi_{|x|}(x).$$

Hence (ψ_n) is contained in #P/poly. □

In fact, it is not hard to see that the conclusion of the lemma is also valid if $(\varphi_n) \in$ #P/poly.

We define the *weight* $\mathrm{wt}(f)$ of a polynomial $f \in \mathbb{Z}[X_1,\ldots,X_n]$ as the sum of the absolute values of its coefficients. It is easy to check that the weight is subadditive and submultiplicative:

$$\mathrm{wt}(f+g) \leqslant \mathrm{wt}(f) + \mathrm{wt}(g), \quad \mathrm{wt}(f \cdot g) \leqslant \mathrm{wt}(f) \cdot \mathrm{wt}(g).$$

Let Γ be a straight-line program using the operations $+, -, *$. Each node ρ in the acyclic digraph associated with Γ has a *multiplicative depth* $d_*(\rho)$, which is defined similarly as the usual depth, but only multiplication nodes are counted. Analogously,

we define the *additive depth* $d_+(\rho)$ (counting only additions and subtractions). The multiplicative and additive depth of Γ are defined as the maximum of the numbers $d_*(\rho)$ and $d_+(\rho)$ taken over all ρ, respectively.

Lemma 2.4. *Let $f \in \mathbb{Z}[X_1,\ldots,X_n]$ be computed by a straight-line program Γ from the variables X_i and integers of absolute value at most $b \geqslant 2$. Then we have*

$$\deg f \leqslant 2^{d_*},\ \log \mathrm{wt}(f) \leqslant (d_+ + 1)\, 2^{d_*} \log b,$$

where d_* and d_+ denote the multiplicative and additive depth of Γ.

Proof. Let (g_ρ) be the result sequence of Γ. We prove by induction on ρ that

$$\log \mathrm{wt}(g_\rho) \leqslant (d_+(\rho) + 1)\, 2^{d_*(\rho)} \log b.$$

If $g_\rho = g_i \cdot g_j$ with $i,j<\rho$, then $d_*(\rho) = 1 + \max\{d_*(i), d_*(j)\}$ and $d_+(\rho) = \max\{d_+(i), d_+(j)\}$. We thus have

$$\begin{aligned}\log \mathrm{wt}(g_\rho) &\leqslant \log \mathrm{wt}(g_i) + \log \mathrm{wt}(g_j)\\ &\leqslant 2\,(d_+(\rho)+1) \max\{2^{d_*(i)}, 2^{d_*(j)}\} \log b\\ &= (d_+(\rho)+1)\, 2^{d_*(\rho)} \log b.\end{aligned}$$

If $g_\rho = g_i + g_j$, $i,j<\rho$, then $d_*(\rho) = \max\{d_*(i), d_*(j)\}$ and $d_+(\rho) = 1 + \max\{d_+(i), d_+(j)\}$. Hence

$$\begin{aligned}\log \mathrm{wt}(g_\rho) &\leqslant 1 + \max\{\log \mathrm{wt}(g_i), \log \mathrm{wt}(g_j)\}\\ &\leqslant 1 + d_+(\rho)\, 2^{d_*(\rho)} \log b \leqslant (d_+(\rho)+1)\, 2^{d_*(\rho)} \log b.\end{aligned}$$

The induction start is clear, and the proof of the degree estimate is left to the reader. □

For later use, we also note the following important result on efficient parallelization of straight-line programs.

Theorem 2.5 (Valiant et al. [26]). *Let f be an n-variate polynomial of degree $d \geqslant 1$ over k with complexity $L(f)$. Then f can be computed by a straight-line program of size $\mathrm{O}(d^6 L(f)^3)$ and depth $\mathrm{O}(\log(dL(f)) \log d + \log n)$.*

3. Relating NP to counting classes

In order to deduce Corollary 1.2 from Theorem 1.1 over finite fields, we need the following result.

Theorem 3.1. *For a prime p we have*

$$\mathrm{NP/poly} \subseteq \mathrm{Mod}_p\mathrm{NP/poly}.$$

Proof. We denote by $\#\phi$ the number of satisfying assignments of a Boolean formula ϕ. It is sufficient to find a function mapping a conjunctive normal form (cnf) ϕ to a cnf χ such that

$$\#\phi > 0 \Leftrightarrow \#\chi \equiv 1 \bmod p. \tag{1}$$

The map $\phi \mapsto \chi$ should be moreover computable in nonuniform polynomial time. □

The easy proof of the following lemma is left to the reader.

Lemma 3.2. *Let ϕ and ψ be cnfs in the disjoint set of variables $X_1,\ldots,X_m$ and $Y_1,\ldots,Y_n$.*

(1) $\#(\phi \wedge \psi) = \#\phi \cdot \#\psi$.

(2) *The formula $\sigma := (Z \to \phi) \wedge \bigwedge_{j=1}^{n}(Z \to Y_j) \wedge (\bar{Z} \to \psi) \wedge \bigwedge_{i=1}^{m}(\bar{Z} \to X_i)$ satisfies $\#\sigma = \#\phi + \#\psi$. It can be transformed into an equivalent cnf in polynomial time.*

(3) *From the cnf ϕ and $t \in \mathbb{N}$ (given in binary), we can compute in polynomial time a cnf ϕ_t satisfying $\#\phi_t = t$.*

(4) *From cnfs $\Phi_1,\ldots,\Phi_q$ and a prime p we can compute in polynomial time a cnf χ such that*

$$\#\chi = 1 + \prod_{j=1}^{q}(p - 1 + \#\Phi_j).$$

Our proof of Theorem 3.1 heavily relies on the reduction in Valiant and Vazirani [27]. They showed that one can assign to a cnf ϕ in n variables and to a random bitstring w of length n a cnf Φ such that

$$\#\phi = 0 \Rightarrow \#\Phi = 0, \quad \#\phi > 0 \Rightarrow \mathrm{Prob}[\#\Phi \neq 1] \leqslant 1 - (4n)^{-1}.$$

Moreover, the map $(\phi, w) \mapsto \Phi$ is computable in polynomial time.

Let now a cnf ϕ with n variables and an odd natural number q be given. Choose q random bitstrings $w_1,\ldots,w_q$ of length n. Let Φ_i be the cnf assigned to ϕ and w_i by the reduction of Valiant and Vazirani. Further, let χ be the cnf corresponding to $\Phi_1,\ldots,\Phi_q$ (and the fixed prime p) according to Lemma 3.2(4). Then χ can be computed from $(\Phi, w_1,\ldots,w_q)$ in polynomial time. Moreover, we have

$$\#\phi = 0 \Rightarrow \#\chi \equiv 0 \bmod p, \quad \#\phi > 0 \Rightarrow \mathrm{Prob}[\#\chi \not\equiv 1 \bmod p] \leqslant (1 - (4n)^{-1})^q.$$

Now we proceed with "Adleman's trick" [1]. Let N_a be the number of cnfs of size $a \geqslant n$. It is easy to see that $\log N_a = a^{O(1)}$. If we choose $q = a^{O(1)}$ big enough, then

$$N_a(1 - (4n)^{-1})^{nq/n} \leqslant N_a \mathrm{e}^{-q/4n} < 1.$$

This implies that for each a there exist $w_1,\ldots,w_q$ such that for *all* cnfs ϕ of size a we have

$$\#\phi > 0 \Rightarrow \#\chi \equiv 1 \bmod p.$$

The bitstrings $w_1,\ldots,w_q$ then serve as an advice to the cnfs of size a. This proves the claim (1) and thus the theorem. □

We deduce now Corollary 1.2 from Theorem 1.1. Assume we had $\mathrm{VP}_k = \mathrm{VNP}_k$. For $\mathrm{char}\, k = 0$ we then obtain from Theorem 1.1 under (GRH) that

$$\#\mathrm{P/poly} \subseteq \mathrm{BP}(\mathrm{VNP}_k) = \mathrm{BP}(\mathrm{VP}_k) \subseteq \mathrm{FNC}^3/\mathrm{poly} \subseteq \mathrm{FP/poly} \subseteq \#\mathrm{P/poly},$$

thus we have equality everywhere. In particular, $\mathrm{P/poly} = \mathrm{NP/poly}$. It is well-known that $\mathrm{P} = \mathrm{NP}$ implies $\mathrm{P} = \mathrm{PH}$ (cf. [12]). A similar argument shows that $\mathrm{P/poly} = \mathrm{NP/poly}$ implies $\mathrm{P/poly} = \mathrm{PH/poly}$. Moreover, by Karp and Lipton [13], the statement $\mathrm{P/poly} = \mathrm{NP/poly}$ implies the collapse of the polynomial hierarchy at the second level.

In the case of a finite field k of characteristic p we argue as follows. If $\mathrm{VP}_k = \mathrm{VNP}_k$, we get from Theorem 1.1 as above

$$\#_p\mathrm{P/poly} \subseteq \mathrm{FNC}^2/\mathrm{poly} \subseteq \mathrm{FP/poly}.$$

Switching to the corresponding classes of languages we obtain

$$\mathrm{Mod}_p\mathrm{NP/poly} \subseteq \mathrm{NC}^2/\mathrm{poly} \subseteq \mathrm{P/poly} \subseteq \mathrm{NP/poly}.$$

By invoking Theorem 3.1 we see that we have equality in the above chain of inclusions. □

4. Reduction modulo primes

Let $f_1,\ldots,f_s \in \mathbb{Z}[X_1,\ldots,X_n]$ be polynomials of degree and weight bounded by $d \geqslant n$ and w, respectively. We assume that the system of equations

$$(S) \qquad f_1 = 0,\ f_2 = 0,\ldots,f_s = 0$$

is solvable over $\mathbb{C}$. Let $\pi(x)$ denote the number of primes $\leqslant x$, and let $\pi_S(x)$ stand for the number of primes $p \leqslant x$ such that (S) is solvable over the finite field $\mathbb{F}_p$.

The goal of this section is to deduce the following improvement of Theorem 8 in Koiran [16], which is of considerable interest in its own right.

Theorem 4.1. *Assuming the generalized Riemann hypothesis (GRH), we have*

$$\pi_S(x) \geqslant \frac{\pi(x)}{d^{\mathrm{O}(n)}} - x^{1/2}\log(wx)$$

for all systems (S) solvable over $\mathbb{C}$.

4.1. A bound on the heights

The first ingredient of the proof of Theorem 4.1 is an estimate of the heights of solutions of the system (S), which we are going to derive in the sequel.

Lemma 4.2. *Let $U_1,\dots,U_t$ be proper linear subspaces of $\mathbb{Q}^{s+1}$ and let $\Sigma_s(t)=\{a\in\mathbb{N}^{s+1}\mid\sum_{\sigma=0}^{s}a_\sigma=t\}$ be the set of lattice points of an s-dimensional simplex. Then we have*

$$\Sigma_s(t)\not\subseteq U_1\cup U_2\cup\cdots\cup U_t.$$

Proof. We proceed by induction on $s+t$. The start is clear. For the induction step we distinguish two cases. Assume first that $\mathbb{Q}^s\times\{0\}$ is not contained in any of the U_τ. Then the U'_τ defined by $U'_\tau\times\{0\}=U_\tau\cap(\mathbb{Q}^s\times\{0\})$ are proper linear subspaces of $\mathbb{Q}^s$, and we have by the induction hypothesis

$$\Sigma_{s-1}(t)\not\subseteq U'_1\cup\cdots\cup U'_t,$$

hence $\Sigma_s(t)\not\subseteq U_1\cup\cdots\cup U_t$. If $\mathbb{Q}^s\times\{0\}$ equals one of the U_τ, say U_t, then we get

$$\Sigma_s(t-1)\simeq\Sigma_s(t)\cap\{a_s>0\}\not\subseteq U_1\cup\cdots\cup U_{t-1}$$

by the induction hypothesis. Therefore $\Sigma_s(t)\not\subseteq U_1\cup\cdots\cup U_t$. □

We remark that the lemma is optimal in the sense that $t+1$ proper linear subspaces are sufficient to cover $\Sigma_s(t)$.

In what follows, let δ denote the codimension of the zeroset $Z(f_1,\dots,f_s)$ in $\mathbb{C}^n$.

Lemma 4.3. *There exist $a_{i\sigma}\in\mathbb{N}$ for $1\leqslant i\leqslant\delta$, $1\leqslant\sigma\leqslant s$, such that the zeroset of the polynomials*

$$F_i=\sum_{\sigma=1}^{s}a_{i\sigma}f_\sigma,\quad 1\leqslant i\leqslant\delta,$$

has codimension δ in $\mathbb{C}^n$, and such that $\sum_{\sigma=1}^{s}a_{i\sigma}\leqslant d^{\delta-1}$.

Proof. Assume we have already constructed $F_1,\dots,F_r$ such that the codimension of the zeroset W of these polynomials equals $r<\delta$. Let $C_1,\dots,C_t$ be the irreducible components of W of (maximal) dimension $n-r$. By Bézout's inequality (cf. [7, 8.28]), we know that $t\leqslant\sum_{\tau=1}^{t}\deg C_\tau\leqslant d^r\leqslant d^{\delta-1}$. The linear spaces

$$U_\tau:=\left\{a\in\mathbb{Q}^s\,\middle|\,\sum_{\sigma=1}^{s}a_\sigma f_\sigma\ \text{vanishes on}\ C_\tau\right\}$$

are proper subspaces of $\mathbb{Q}^s$, since otherwise C_τ would be contained in the zeroset of $f_1,\dots,f_s$, which implied the contradiction $r=\operatorname{codim}C_\tau\geqslant\delta$. By Lemma 4.2, there exists $a\in\mathbb{N}^s$ satisfying $a\notin U_1\cup\cdots\cup U_t$ and $\sum_{\sigma=1}^{s}a_\sigma=t$. We define $F_{r+1}:=\sum_{\sigma=1}^{s}a_\sigma f_\sigma$ and obtain $\operatorname{codim}Z(F_1,\dots,F_{r+1})=r+1$ as desired. □

We note that Lemma 4.3 implies the following (well known) fact: if $C_1,\dots,C_t$ are the irreducible components of $Z(f_1,\dots,f_s)$ of maximal dimension, then

$$\sum_{\tau=1}^{t}\deg C_\tau\leqslant d^\delta. \tag{2}$$

Lemma 4.4. *There exist affine linear polynomials* $g_1,\ldots,g_{n-\delta}$ *such that the zeroset* $Z(f_1,\ldots,f_s,g_1,\ldots,g_{n-\delta})$ *is zero-dimensional and* $\mathrm{wt}(g_\mu)\leqslant d^{n-1}+1$.

Proof. Assume we have already constructed $g_1,\ldots,g_m$, $m<n-\delta$, such that $W:=Z(f_1,\ldots,f_s,g_1,\ldots,g_m)$ has codimension $\delta+m$. Let $C_1,\ldots,C_t$ be the irreducible components of W of maximal dimension. By observation (2) we know that $\sum_{\tau=1}^{t}\deg C_\tau \leqslant d^{\delta+m}$.

We need to prove the existence of a "small" nonzero $a\in\mathbb{N}^{n+1}$ such that the affine hyperplane $H:=Z(a_0+\sum_{i=1}^{n}a_iX_i)$ has a nonempty intersection with W, but does not contain any of the C_τ. For this, it is convenient to take a projective point of view. Think of $\mathbb{C}^n$ as being embedded in $\mathbb{P}^n$ and let $\mathscr{H}$ be the Grassmannian consisting of the hyperplanes in $\mathbb{P}^n$. Note that $\mathscr{H}$ can be naturally identified with $\mathbb{P}^n$ itself.

There is a a curve K contained in C_1 such that $\deg K\leqslant\deg C_1$. (Just intersect C_1 with an affine subspace of complementary dimension which is in general position, and apply Bézout's inequality.) Let $\bar{K}$ be the projective closure of K. Then we have $\bar{K}=K\cup K_\infty$, where K_∞ is the finite set of points of $\bar{K}$ at infinity. By Bézout's inequality, we have $|K_\infty|\leqslant\deg K$. For $p\in\mathbb{P}^n$ consider the hyperplanes

$$\mathscr{V}_p:=\{H\in\mathscr{H}\mid p\in H\}$$

in $\mathscr{H}$. If some $H\in\mathscr{H}$ does not intersect W, then it does not intersect the affine part K of $\bar{K}$, hence it must intersect $\bar{K}$ in one of its points at infinity. To put it differently: any hyperplane H lying in none of the $\mathscr{V}_p$, $p\in K_\infty$, must necessarily intersect W.

Consider now the following proper linear subspaces of $\mathscr{H}$

$$\mathscr{U}_\tau:=\{H\in\mathscr{H}\mid C_\tau\subseteq H\}.$$

Lemma 4.2 shows the existence of some $a\in\mathbb{N}^{n+1}$ such that the hyperplane $H=Z(\sum_{i=0}^{n}a_iX_i)$ satisfies

$$H\notin\bigcup_{\tau=1}^{t}\mathscr{U}_\tau\cup\bigcup_{p\in K_\infty}\mathscr{V}_p$$

and $\sum_{i=0}^{n}a_i=t+|K_\infty|$. (To obtain this, interpret the $\mathscr{U}_\tau$ and $\mathscr{V}_p$ as linear subspaces of $\mathbb{C}^{n+1}$). Since

$$\begin{aligned}t+|K_\infty| &\leqslant t+\deg C_1\leqslant\deg C_1+\cdots\deg C_t+1\\ &\leqslant d^{\delta+m}+1\leqslant d^{n-1}+1,\end{aligned}$$

this proves the assertion. □

Let (S) be a system of equations as introduced at the beginning of Section 4. Based on a result in Krick and Pardo [17, 18], which itself heavily relies on the techniques in Giusti and Heintz [11], we can now specify a solution of (S) as follows.

Theorem 4.5. *The system* (S) *has a solution* $x=(x_i)$ *of the form* $x_i=\theta^{-1}v_i(y)$. *Here* θ *is a positive integer,* $v_i\in\mathbb{Z}[Y]$ *is an integer polynomial, and* y *is an algebraic number with primitive integer minimal polynomial* $g\in\mathbb{Z}[Y]$ *such that*

$$\max\{\deg g,\deg v_i\}=d^{\mathrm{O}(n)},\ \max\{\log\theta,\log\mathrm{wt}(g),\log\mathrm{wt}(v_i)\}=d^{\mathrm{O}(n)}\log w.$$

Proof. By Lemma 4.4, we can add to the system (S) suitable linear equations of weight at most d^n, such that the resulting system becomes zero-dimensional. By Lemma 4.3, we obtain n integer polynomials $F_1,\dots,F_n$ satisfying $\deg F_i\leqslant d$, $\mathrm{wt}(F_i)\leqslant wd^{2n}$, and such that $V:=Z(F_1,\dots,F_n)$ is zero-dimensional and contains a solution of the original system (S).

We can now apply Proposition 27 of [18], which claims the existence of an integer linear form $\gamma=\gamma_1X_1+\cdots+\gamma_nX_n$, of a positive integer θ, and of univariate integer polynomials $v_i\in\mathbb{Z}[Y]$, $1\leqslant i\leqslant n$, such that the following holds:

(1) The linear form γ separates the points of V.
(2) We have $\theta x_i=v_i(\gamma(x))$ for all $x=(x_1,\dots,x_n)\in V$.
(3) $\mathrm{wt}(\gamma)=d^{\mathrm{O}(n)}$.
(4) Both θ and the coefficients of the v_i are integer polynomials in the coefficients of $F_1,\dots,F_n$, and they can be evaluated from these coefficients and the constant 1 by a division-free straight-line program of size $d^{\mathrm{O}(n)}$ and multiplicative depth $\mathrm{O}(n\log d)$.

(The original statement in [18, Proposition 27] is about nonscalar straight-line programs, but it is easily seen to be equivalent to our formulation.)

Taking into account that the coefficients of F_i are bounded by wd^{2n}, we conclude with Lemma 2.4 that

$$\deg v_i=d^{\mathrm{O}(n)},\quad \max\{\log\theta,\log\mathrm{wt}(v_i)\}=d^{\mathrm{O}(n)}\log w.$$

Choose $x\in V$ and set $y:=\gamma(x)$. Let g be a minimal polynomial of y, which we moreover assume to be a primitive integer polynomial. We need to show the desired estimates of the degree and weight of g. Consider the univariate integer polynomials

$$G_i(Y):=\theta^dF_i(\theta^{-1}v_1(Y),\dots,\theta^{-1}v_n(Y)).$$

We may assume that at least one of the G_i is nonzero, since otherwise all v_i are constant, and we are done already. Note that $G_i(y)=0$ for all i. Hence g is a divisor of G_i in $\mathbb{Z}[Y]$. Now we are going to bound the degree and weight of G_i. Write $F_i=\sum_\mu c_\mu X_1^{\mu_1}\cdots X_n^{\mu_n}$. Then we have

$$G_i=\sum_\mu c_\mu\theta^{d-|\mu|}v_1^{\mu_1}\cdots v_n^{\mu_n},$$

hence $\deg G_i\leqslant\deg F_i\cdot\max_i\deg v_i=d^{\mathrm{O}(n)}$. Using the subadditivity and submultiplicativity of the weight we infer that $\mathrm{wt}(G_i)\leqslant\theta^d\mathrm{wt}(F_i)(\max_i\mathrm{wt}(v_i))^d$, which implies $\log\mathrm{wt}(G_i)=d^{\mathrm{O}(n)}\log w$.

The bound in Mignotte [21] on the coefficients of divisors of polynomials

$$\mathrm{wt}(g)\leqslant\frac{\mathrm{lc}(g)}{\mathrm{lc}(G_i)}2^{\deg g}\|G_i\|$$

implies the desired estimate of $\mathrm{wt}(g)$. (Here, $\mathrm{lc}(g)$ denotes the leading coefficient of g and $\|G_i\|$ is the L_2-norm of the coefficient vector of G_i.) $\square$

Remark 4.6. We adopt the notation of Theorem 4.5. Let $\bar{y}$ be a root of g in $\mathbb{F}_p$ and assume that p is not a factor of θ. Consider the integer polynomials

$$h_i(Y) := \theta^d f_i(\theta^{-1}v_1(Y), \ldots, \theta^{-1}v_n(Y)).$$

As $(\theta^{-1}v_i(y))_i$ is a solution of (S), we have $h_i(y) = 0$. Therefore, the minimal polynomial g is a factor of h_i in $\mathbb{Q}[Y]$. Since we assume g to be primitive, it is even a factor of h_i in $\mathbb{Z}[Y]$. By our assumption, we have $g(\bar{y}) = 0$ in $\mathbb{F}_p$. Hence $h_i(\bar{y}) = 0$ and we conclude that $(\theta^{-1}v_i(\bar{y}))_i$ is a solution of (S) over $\mathbb{F}_p$.

So it remains to investigate the distribution of the roots mod p of univariate polynomials. This will be done in the next subsection.

4.2. Roots of univariate polynomials modulo a prime

Let g be an irreducible univariate integer polynomial of degree d. It is well known that there is a bijection between the irreducible factors of g modulo p and the primes of the number field $K = \mathbb{Q}[Y]/(g)$ lying over p, provided p is not a divisor of the discriminant Δ of g (cf. [20]). Under this bijection, the roots of g modulo p correspond to the primes of degree one lying over p. Let $\pi_K(x)$ denote the number of primes of K having norm at most x, and $\mathrm{li}(x) = \int_2^x \mathrm{d}u/\ln u \sim x/\ln x$ be the logarithmic integral. It is known that under a generalized Riemann hypothesis (GRH) the following effective version of the "prime number theorem" for number fields is true (Weinberger [28], see also Lagarias and Odlyzko [19]):

$$|\pi_K(x) - \mathrm{li}(x)| = \mathrm{O}(x^{1/2}\log(|\Delta|x^d)). \tag{3}$$

(The constant implicit in the O-term does not depend on g.) Of course, this contains an effective version of the usual prime number theorem ($K = \mathbb{Q}$) as a special case. We recall that the *generalized Riemann hypothesis* (GRH) claims that all complex roots $s + it$ of ζ_K in the critical strip $0 \leqslant s \leqslant 1$ satisfy $s = \frac{1}{2}$.

A prime ideal of K having norm $\leqslant x$ and degree > 1 lies over a rational prime $p \leqslant x^{1/2}$. Hence there are at most $\mathrm{d}x^{1/2}$ such primes of K. Moreover, there are at most $\log|\Delta|$ prime factors of Δ. By taking into account these considerations, and using also the effective prime number theorem for $\mathbb{Q}$, one can easily deduce from (3) the following result (cf. Weinberger [29]).

Theorem 4.7. *Let $g \in \mathbb{Z}[Y]$ be irreducible with degree d and discriminant Δ. Then the total number $N_g(x)$ of roots of g modulo all the primes up to x satisfies*

$$|N_g(x) - \pi(x)| = \mathrm{O}(x^{1/2}\log(|\Delta|x^d) + d\,\log|\Delta|),$$

provided (GRH) is true.

Let $\pi_g(x)$ stand for the number of primes $p \leqslant x$ such that g has a root modulo p. It is obvious that $N_g(x) \leqslant d\,\pi_g(x)$. Moreover, if w is an upper bound on the weight of g, then we have the estimate $\log|\Delta| = \mathrm{O}(d\log(dw))$ for the discriminant Δ. Taking these observations into account, we obtain the following corollary.

Corollary 4.8. *For all irreducible univariate polynomials $g \in \mathbb{Z}[Y]$ of degree d and weight w we have*

$$\pi_g(x) \geqslant \frac{\pi(x)}{d} - \mathrm{O}(x^{1/2}\log(dwx) + d\log(dw)),$$

provided (GRH) is true.

The proof of Theorem 4.1 follows now easily by combining Theorem 4.5, Remark 4.6, and Corollary 4.8.

5. Proof of Theorem 1.1

(A) We first discuss the more complicated case where $\operatorname{char} k = 0$.

(A1) $\mathrm{FNC}^1/\mathrm{poly} \subseteq \mathrm{BP}(\mathrm{VP}_k)$:

Let (C_n) be a sequence of Boolean circuits of size $s_n = n^{\mathrm{O}(1)}$ and depth $d_n = \mathrm{O}(\log n)$ and φ_n be the function computed by C_n. Using the relations

$$\forall x, y \in \{0,1\}\colon x \wedge y = x\cdot y,\ \neg x = 1 - x,\ x \vee y = x + y - x\cdot y$$

we can simulate C_n by a straight-line program Γ_n of size $\leqslant 3s_n$ and depth $\leqslant 2d_n$. If $g_{n,i}$ are the polynomials computed by Γ_n, we have $g_{n,i}(x) = \varphi_{n,i}(x)$ for all $x \in \{0,1\}^n$. Thus (φ_n) is a Boolean part of (f_n) defined by $f_n := \sum_{i=1}^{m(n)} g_{n,i}2^{i-1}$. The family (f_n) is p-computable, since its degree is growing at most polynomially due to

$$\deg g_n \leqslant 2^{\operatorname{depth}\Gamma_n} \leqslant n^{\mathrm{O}(1)}.$$

(A2) $\#\mathrm{P}/\mathrm{poly} \subseteq \mathrm{BP}(\mathrm{VNP}_k)$:

Let (φ_n) be a string function in #P and set $\phi(x) := \sum_i \varphi_{n,i}(x)2^{i-1}$ for $x \in \{0,1\}^n$. By our definition $\phi : \{0,1\}^* \to \mathbb{N}$ is also in #P, hence there is a polynomial-time nondeterministic Turingmachine M such that $\phi(x)$ equals the number of accepting computations of M on x for all $x \in \{0,1\}^*$. The proof of Cook's theorem [8] shows that for each $n \in \mathbb{N}$ there is a 3-conjunctive normal form Φ_n in the variables $X_1,\ldots,X_n, Y_1,\ldots,Y_{m(n)}$, $m(n) = n^{\mathrm{O}(1)}$, having $n^{\mathrm{O}(1)}$ clauses, such that

$$\phi(x) = \#\{y \in \{0,1\}^{m(n)} \mid \Phi_n(x,y) \text{ true}\}.$$

It is easy to see that for each 3-clause K there is a polynomial g_K in three variables of degree $\leqslant 3$ and with coefficients of size $\mathrm{O}(1)$ such that

$$\forall e \in \{0,1\}^3\colon g_K(e) = \begin{cases} 1 & \text{if } K(e) \text{ true,} \\ 0 & \text{otherwise.} \end{cases}$$

(For instance, for $K = u \vee v \vee w$ take $g_K := uvw + uv(1-w) + u(1-v)w + (1-u)vw + u(1-v)(1-w) + (1-u)v(1-w) + (1-u)(1-v)w$.)

Let f_n be the product of the g_K over all clauses K of Φ_n. Clearly, (f_n) is p-computable. Now define the p-definable family (g_n) by

$$g_n(X) := \sum_{y \in \{0,1\}^{m(n)}} f_n(X, y).$$

Then we have $g_n(x) = \phi(x)$ for all $x \in \{0,1\}^n$. Therefore, (φ_n) is a Boolean part of (g_n). This shows that $\#\mathrm{P} \subseteq \mathrm{BP}(\mathrm{VNP}_k)$.

Now let (ψ_n) be in $\#\mathrm{P}/\mathrm{poly}$. By definition, there is some (φ_n) in $\#\mathrm{P}$ and some polynomial advice function α such that for all $x \in \{0,1\}^n$

$$\psi_n(x) = \varphi_{t(n)}(\langle x, \alpha(n)\rangle),$$

where $t(n) = 2n + 2|\alpha(n)| + 2$ is the length of $\langle x, \alpha(n)\rangle$. By the reasoning before, there exists $(g_n) \in \mathrm{VNP}_k$ such that $g_n(x) = \sum_i \varphi_{n,i}(x) 2^{i-1}$ for $x \in \{0,1\}^n$. Now define the polynomial $h_n(X) := g_{t(n)}(\langle X, \alpha(n)\rangle)$ (the pairing has the obvious meaning). (h_n) is p-definable as it is a p-projection of (g_n). On the other hand, we have for all $x \in \{0,1\}^n$

$$h_n(x) = g_{t(n)}(\langle x, \alpha(n)\rangle) = \sum_i \varphi_{t(n),i}(\langle x, \alpha(n)\rangle)\, 2^{i-1} = \sum_i \psi_{n,i}(x) 2^{i-1}.$$

Therefore, (ψ_n) is a Boolean part of (h_n) and hence $(\psi_n) \in \mathrm{BP}(\mathrm{VNP}_k)$.

(A3) $\mathrm{BP}(\mathrm{VP}_k) \subseteq \mathrm{FNC}^3/\mathrm{poly}$:

Assume $(f_n) \in \mathrm{VP}_k$ has a Boolean part. Hence there is some p-bounded function $t : \mathbb{N} \to \mathbb{N}$ such that $f_n(x) < 2^{t(n)}$ for $x \in \{0,1\}^n$. By Theorem 2.5 there is for each n some straight-line program Γ_n of size $n^{\mathrm{O}(1)}$ and depth $\mathrm{O}(\log^2 n)$ which computes f_n from $X_1, \ldots, X_n$ and *constants* $y_1, \ldots, y_{m(n)}$ in k. (In particular, $m(n) = n^{\mathrm{O}(1)}$.) Replace the y_j by indeterminates Y_j and let $F_n(X, Y)$ denote the integer polynomial computed by Γ_n from the X_i and Y_j. We conclude from Lemma 2.4 that

$$\deg F_n \leqslant 2^{\mathrm{O}(\log^2 n)}, \quad \log \mathrm{wt}(F_n) \leqslant 2^{\mathrm{O}(\log^2 n)}.$$

Obviously, $F_n(X, y) = f_n$, hence the system of equations

$$F_n(x, Y) - f_n(x) = 0 \quad \text{for all } x \in \{0,1\}^n \tag{S_n}$$

has a solution $y \in k^{m(n)}$. By the Nullstellensatz, the system (S_n) is also solvable over the algebraic closure of $\mathbb{Q}$ and thus over $\mathbb{C}$.

Note that $\mathrm{wt}(F_n(x, Y)) \leqslant \mathrm{wt}(F_n)$ for $x \in \{0,1\}^n$. Hence the degree as well as the logarithm of the weight of the polynomials in (S_n) are bounded by $2^{\mathrm{O}(\log^2 n)}$. Theorem 4.1 implies that for a suitable constant $c > 0$

$$\pi_{S_n}(2^{n^c}) > 2^{t(n)}$$

for sufficiently large n. Therefore, there is some prime number p_n satisfying $t(n) < \log p_n \leqslant n^c$ such that (S_n) is solvable over $\mathbb{F}_{p_n}$. Let $\bar{y}_n \in \mathbb{F}_{p_n}^{m(n)}$ denote such a solution.

We remark that the addition and multiplication in $\mathbb{F}_p$ can be performed by (uniform) Boolean circuits of size $(\log p)^{O(1)}$ and depth $O(\log\log p)$ (cf. Karp and Ramachandran [14, Section 4.2.2]). Using this, we see that we can simulate the straight-line program Γ_n in $\mathbb{F}_{p_n}$ with constants $\bar{y}_n$ by a Boolean circuit C_n satisfying

$$\operatorname{size}(C_n) = (\log p_n)^{O(1)} \cdot \operatorname{size}(\Gamma_n) = n^{O(1)},$$
$$\operatorname{depth}(C_n) = O(\log\log p_n \cdot \operatorname{depth}(\Gamma_n)) = O(\log^3 n).$$

The circuit C_n computes a bit representation of $F_n(x, \bar{y}_n) \in \mathbb{F}_{p_n}$ on input $x \in \{0,1\}^n$. (We can think of p_n and $\bar{y}_n$ as being "hard-wired" in C_n.) Since

$$f_n(x) \bmod p_n = F_n(x, \bar{y}_n)$$

and $f_n(x) < 2^{t(n)} \leqslant p_n$, C_n actually computes a bit representation of $f_n(x)$.

(A4) $\mathrm{BP}(\mathrm{VNP}_k) \subseteq \mathrm{FP}^{\#\mathrm{P}}/\mathrm{poly}$:

Assume $(f_n) \in \mathrm{VNP}_k$ has a Boolean part. By definition, there is a p-computable family (g_n) and a p-bounded function $u : \mathbb{N} \to \mathbb{N}$ such that

$$f_n = \sum_{e \in \{0,1\}^{u(n)-n}} g_{u(n)}(X_1, \ldots, X_n, e_{n+1}, \ldots, e_{u(n)}). \tag{4}$$

Under the additional assumption that also (g_n) has a Boolean part (φ_n), we could easily finish the argumentation. By the inclusion (A3) just proved before, we had $(\varphi_n) \in \mathrm{FNC}^3/\mathrm{poly} \subseteq \mathrm{FP}/\mathrm{poly}$. Therefore, we would have for all $x \in \{0,1\}^n$

$$f_n(x) = \sum_e g_{u(n)}(x, e) = \sum_{e,i} \varphi_{u(n),i}(x, e) 2^{i-1}$$

and Lemma 2.3 would imply that the map $\{0,1\}^* \to \mathbb{N}$, $x \mapsto f_{|x|}(x)$ is in $\#\mathrm{P}/\mathrm{poly}$.

In the general situation, we may argue similarly as in the proof of (A3). Let $t : \mathbb{N} \to \mathbb{N}$ be p-bounded such that $f_n(x) < 2^{t(n)}$ for $x \in \{0,1\}^n$. For each n there is some straight-line program Γ_n of size $n^{O(1)}$ and depth $O(\log^2 n)$ which computes g_n from indeterminates $X_1, \ldots, X_n, E_{n+1}, \ldots, E_{u(n)}$ and constants $y_1, \ldots, y_{m(n)}$ in k. Let $G_n(X, E, Y)$ be the integer polynomial computed by Γ_n if we replace the y_j by indeterminates Y_j. It is clear that $g_n = G_n(X, E, y)$. We will apply Theorem 4.1 to the system

$$\sum_{e \in \{0,1\}^{u(n)-n}} G_{u(n)}(x, e, Y) - f_n(x) = 0 \quad \text{for all } x \in \{0,1\}^n, \tag{S'_n}$$

which is solvable over $\mathbb{C}$. Note that

$$\operatorname{wt}\left(\sum_e G_{u(n)}(x, e, Y)\right) \leqslant \sum_e \operatorname{wt}(G_{u(n)}) \leqslant 2^{2^{O(\log^2 n)}}.$$

Hence the degree as well as the logarithm of the weight of the polynomials in (S'_n) are bounded by $2^{O(\log^2 n)}$. By Theorem 4.1 there is some prime number $p_n \geqslant 2^{t(n)}$ of bitsize $n^{O(1)}$ such that (S'_n) has a solution $\bar{y}_n \in \mathbb{F}_{p_n}^{m(n)}$.

As in (A3), we can construct for each n a Boolean circuit C_n of size $n^{O(1)}$ and depth $O(\log^3 n)$ which computes from $(x,e)\in\{0,1\}^{u(n)}$ the bit representation of a natural number $\varphi_{u(n)}(x,e)$ such that

$$\psi_n(x) := \sum_{e\in\{0,1\}^{u(n)-n}} \varphi_{u(n)}(x,e)$$

satisfies $\psi_n(x) \bmod p_n = f_n(x)$. The map $\psi:\{0,1\}^*\to\mathbb{N},\ x\mapsto\psi_{|x|}(x)$ is in #P/poly by Lemma 2.3. Hence $\{0,1\}^*\to\mathbb{N},\ x\mapsto f_{|x|}(x)$ is in $\mathrm{FP}^{\#\mathrm{P}}$/poly.

(B) Let now $k=\mathbb{F}_{p^e}$ be a finite field with p^e elements. We can represent the elements of k by bit vectors using the isomorphism $k\simeq\mathbb{F}_p[T]/(h)$ for some irreducible polynomial h over $\mathbb{F}_p$ of degree e. The arithmetic in k can be very efficiently simulated by Boolean circuits; however, for our purposes, any simulation will do.

Our proofs for (A1) and (A2) can be immediately translated to show the inclusions $\mathrm{FNC}^1/\mathrm{poly}\subseteq\mathrm{BP}(\mathrm{VP}_k)$ and $\#_p\mathrm{P}/\mathrm{poly}\subseteq\mathrm{BP}(\mathrm{VNP}_k)$.

To prove $\mathrm{BP}(\mathrm{VP}_k)\subseteq\mathrm{FNC}^2/\mathrm{poly}$ we start as in (A3) with straight-line programs Γ_n of size $n^{O(1)}$ and depth $O(\log^2 n)$ using constants in k. As k is finite, Γ_n can be directly simulated by Boolean circuits of size $n^{O(1)}$ and depth $O(\log^2 n)$.

In order to show $\mathrm{BP}(\mathrm{VNP}_k)\subseteq\#_p\mathrm{P}$ we assume that $f_n\in\mathbb{F}_p[X_1,\ldots,X_n]$ has a representation as in (4) with some $(g_n)\in\mathrm{VP}_k$. Let $b_1=1,\ b_2,\ldots,b_e$ be a basis of k over $\mathbb{F}_p$ and write $g_n(x,e)=\sum_i g_{n,i}(x,e)b_i$ with $g_{n,i}(x,e)\in\mathbb{F}_p$. It is easy to see that $f_n(x)=\sum_e g_{n,1}(x,e)$. A Boolean circuit of size $n^{O(1)}$ can be constructed which computes a bit representation of $g_{n,1}(x,e)$ from x,e. Lemma 2.3 shows now that $x\mapsto f_{|x|}(x)$ is in #P/poly. □

Acknowledgments

I thank Luis Miguel Pardo for pointing out to me that Koiran's method [16] can be improved using the results of [17, 18].

References

[1] L. Adleman, Two theorems on random polynomial time, Proceedings of the 19th IEEE Symposium on Foundations of Comp. Science, 1978, pp. 75–83.

[2] L. Babai, L. Fortnow, Arithmetization: a new method in structural complexity theory, Comp. Compl. 1 (1991) 41–66.

[3] L. Blum, F. Cucker, M. Shub, S. Smale, Algebraic Settings for the Problem "$P\neq NP$?", The Mathematics of Numerical Analysis, No. 32, Lectures in Applied Mathematics, American Mathematical Society, Providence, RI, pp. 125–144.

[4] L. Blum, M. Shub, S. Smale, On a theory of computation and complexity over the real numbers, Bull. Amer. Math. Soc. 21 (1989) 1–46.

[5] P. Bürgisser, Completeness and Reduction in Algebraic Complexity Theory, Habilitationsschrift Universität Zürich, Algorithms and Computation in Mathematics, Vol. 7, Springer, Berlin, to appear.

[6] P. Bürgisser, On the structure of Valiant's complexity classes, Discrete Mathematics and Theoretical Computer Science 3 (1999) 73–94.

[7] P. Bürgisser, M. Clausen, M.A. Shokrollahi, Algebraic Complexity Theory, Grundlehren der mathematischen Wissenschaften, Vol. 315, Springer, Berlin, 1997.
[8] S.A. Cook, The complexity of theorem proving procedures, Proceedings of the 3rd ACM STOC, 1971, pp. 151–158.
[9] F. Cucker, D.Yu. Grigoriev, On the power of real Turing machines over binary inputs, SIAM J. Comp. 26 (1997) 243–254.
[10] J. von zur Gathen, Feasible arithmetic computations: Valiant's hypothesis, J. Symb. Comp. 4 (1987) 137–172.
[11] M. Giusti, J. Heintz, La détermination des points isolés et de la dimension d'une varieté algébrique peut se faire en temps polynomial, in: D. Eisenbud, L. Robbiano (Eds.), Proceedings Cortona Conference on Computational Algebraic Geometry and Commutative Algebra, Cambridge University Press, Cambridge, 1993.
[12] D.S. Johnson, A catalog of complexity classes, in: J. van Leeuwen (Ed.), Handbook of Theoretical Computer Science, Vol. A, Elsevier, Amsterdam, 1990, pp. 61–161 (Chapter 2).
[13] R.M. Karp, R.J. Lipton, Turing machines that take advice, Logic and Algorithmic: An international Symposium held in honor of Ernst Specker, Monogr. No. 30 de l'Enseign. Math., 1982, pp. 255–273.
[14] R.M. Karp, V. Ramachandran, Parallel algorithms for shared-memory machines, in: J. van Leeuwen (Ed.), Handbook of Theoretical Computer Science, Vol. A, Elsevier, Amsterdam, 1990, pp. 869–941 (Chapter 17).
[15] P. Koiran, A weak version of the Blum–Shub–Smale model, Proceedings of the 34th FOCS, 1993, pp. 486–495.
[16] P. Koiran, Hilbert's Nullstellensatz is in the polynomial hierarchy, J. Compl. 12 (1996) 273–286.
[17] T. Krick, L.M. Pardo, Une approche informatique pour l'approximation diophantienne, C.R. Acad. Sci. Paris 318 (1994) 407–412.
[18] T. Krick, L.M. Pardo, A computational method for diophantine approximation, in: L. González-Vega, T. Recio (Eds.), Proceedings of the MEGA'94, Progress in Mathematics, Vol. 143, Birkhäuser, Basel, 1996, pp. 193–253.
[19] J.C. Lagarias, A.M. Odlyzko, Effective versions of the Chebotarev density theorem, Algebraic Number Fields, Proceedings of the 1975 Durham Symposium, Academic Press, New York, 1977, pp. 409–464.
[20] D.A. Marcus, Number Fields, Springer, Berlin, 1977.
[21] M. Mignotte, Some useful bounds, in: B. Buchberger, G.E. Collins, R. Loos (Eds.), Computer Algebra, Symbolic and Algebraic Computation, Springer, Berlin, 1982, pp. 259–263.
[22] L.G. Valiant, Completeness classes in algebra, Proceedings of the 11th ACM STOC, 1979, pp. 249–261.
[23] L.G. Valiant, The complexity of computing the permanent, Theoret. Comp. Sci. 8 (1979) 189–201.
[24] L.G. Valiant, The complexity of enumeration and reliability problems, SIAM J. Comp. 8 (1979) 410–421.
[25] L.G. Valiant, Reducibility by algebraic projections, Logic and Algorithmic: an International Symposium held in honor of Ernst Specker, Monogr. No. 30 de l'Enseign. Math., 1982, pp. 365–380.
[26] L.G. Valiant, S. Skyum, S. Berkowitz, C. Rackoff, Fast parallel computation of polynomials using few processors, SIAM J. Comp. 12(4) (1983) 641–644.
[27] L.G. Valiant, V.V. Vazirani, NP is as easy as detecting unique solutions, Theoret. Comp. Sci. 47 (1986) 85–93.
[28] P.J. Weinberger, On Euclidean rings of algebraic integers, Analytic Number Theory, Proceedings of the Symposium in Pure Mathematics, American Mathematical Society, Providence, RI, 1972, pp. 321–332.
[29] P.J. Weinberger, Finding the number of factors of a polynomial, J. Algorithms 5 (1984) 180–186.